PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)	Examiner: Mohammad W. Reza
Ibrahim, et al.	)	
	)	Art Unit: 2436
Serial No.: 10/827,218	)	
	)	
Filed: 4/19/04	)	Confirmation No.: 2929
	)	
For: SUBORDINATE TRUSTED PLATFORM MODULE	))	
	)	
Date of Examiner's Answer: September 17, 2009	))	Attorney Docket No.: 200314912-1
	)	

November 16, 2009

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

REPLY BRIEF under 37 CFR §41.41

Dear Sir:

This Reply Brief is timely provided within two months from the mailing date of the Examiner's Answer dated September 17, 2009.

Reply

In response to the Examiner's Answer, dated September 17, Appellant respectfully submits the following reply as permitted under 37 CFR §41.41(a)(1). The Examiner's Answer contained no new grounds of rejection and the present reply contains no new amendment, affidavit or other evidence. Thus a formal Brief is not required. The present reply supplements Appellant's Appeal Brief in view of the Examiner's Answer.

Citations to page numbers from the Examiner's Answer will be referred to as "EA page _".

The rejections under 35 U.S.C. §112, first paragraph and second paragraph, have been withdrawn by the examiner.

I. Whether claims 1-18, 45-46, and 48-49 are unpatentable under 35 U.S.C. 103(a) as being obvious over Challener et al. (U.S. Publ. 2003/0105965), in view of Cromer et al. (US Patent 7,191,464).

Independent Claim 1

Claim 1 recites logic configured to perform cryptographic key maintenance:

> where the cryptographic key maintenance includes migrating a non-migratable storage root key from a root of a key storage hierarchy associated with the trusted platform module associated with the trusted platform

Challener and Cromer, neither individually nor combined, teach or suggest this claim feature. The EA relies on Challener's discussion of a non-migratable storage key (EA page 4 and 10). First, Challener explicitly distinguishes between a "non-migratable storage key" and "a storage root key." In paragraph [0027], Challener states:

> Further, there is one key that is guaranteed to always be loaded inside the chip. It is called the storage root key, and it is an ancestor of every other key the chip can use.
> (Challener, [0027] lines 24-26) [Emphasis added]

Thus when Challener is discussing the non-migratable storage key, this is not the storage root key. Claim 1 explicitly recites "a non-migratable storage root key." The examiner has not identified where the claimed element is found in Challener. Thus, Challener fails to teach or suggest migrating a non-migratable storage root key and fails to establish a prima facie rejection.

Furthermore, claim 1 recites, "migrating a non-migratable storage root key from a root of a key storage hierarchy associated with the trusted platform module associated with the trusted platform." The examiner relies on manual operations performed by a user in which they send a key to a credit card company over the Internet (see [0029, 0030, and 0043]). For example, "[t]he customer contacts a credit card company over the Internet..." [0029] lines 1-2; "[t]he customer will provide to the credit card company the non-migratable public portion of the storage key, K1..." [0030] lines 3-5.

Besides not referring to a storage root key, there is no teaching or suggestion of migrating a non-migratable storage root key from a root of a key storage hierarchy. This is not found in the reference and thus is another reason why Challener fails to establish a prima facie rejection.

The EA cites figure 2, elements 202 and 205 with reference to this feature (EA page 4, lines 1-7). Elements 202 to 205 of figure 2 simply discuss the customer creating a non-migratable key and the customer providing it to the credit card company. It is not surprising that the claimed feature is not found because claim 1 is directed to and recites, "a logic configured to perform cryptographic key maintenance for a trusted platform" whereas Challener describes a human customer using the Internet to contact a credit card company. These are two completely different technologies. Each and every element is not found in the reference and the rejection is improper. The rejection should be reversed.

Claim 1 also recites "...a trusted platform to which the logic is bound in a one-to-one manner..." The EA merely repeats the citation to Cromer col. 4, lines 35-38 as teaching this element (EA page 12, lines 1-2). The interpretation and reliance on Cromer is incorrect.

The cited section in Cromer states, "[a]s is shown, the TPM (Trusted Platform Module) 44' includes a plurality of shadow PCRs 48a' that are linked, one-to-one, to the plurality of boot PCRs 48a." (col. 4, lines 36-38).

Merely reciting the term "one-to-one" is not sufficient to teach or suggest the specifically claimed configuration. Cromer teaches a different configuration: shadow registers linked one-to-one to boot registers. This is not on point with the claimed elements. Thus Cromer fails to teach or suggest the claimed logic bound one-to-one with a trusted platform. The claimed element is not found.

Cromer fails to support the rejection for which it is relied upon. Therefore, the combination of Challener and Cromer fail to teach or suggest each and every claimed element. A prima facie obviousness rejection has not been established and the rejection should be reversed.

The remaining portions of the EA (EA pages 12-13) rely on misinterpretations of the references as explained above and as previously explained in Appellant's appeal brief. Appellant repeats the reasoning submitted in the Appeal Brief. A prima facie anticipation or obviousness rejection has not been established. The rejection should be reversed.

Conclusion

Appellant respectfully maintains all previous arguments, which show the deficiencies in the rejections, along with the additional comments submitted herein. Accordingly, Appellant respectfully requests that the Board of Appeals overturn all rejections and allow all pending claims.

Respectfully submitted,

Peter Kraguljac

Peter Kraguljac (Reg. No. 38,520)

(216) 503-5500

Kraguljac & Kalnay, LLC
4700 Rockside Road
Summit One, Suite 510
Independence, OH 44131